SECURING NARROWBAND WIRELESS COMMUNICATION IN LICENSED BAND

David Kolaja
Bachelor Degree Programme (3), FEEC BUT
E-mail: xkolaj03@stud.feec.vutbr.cz

Supervised by: Radek Fujdiak
E-mail: fujdiak@feec.vutbr.cz

Abstract: With everlasting growth of development of devices in the Internet of Things, there is also a difficulty to keep up with the requirements of security-related topics on such devices. This is no exception for expanding the scale of Low Powered Wide Area Network (LPWAN) devices which communicate over Narrowband IoT. Such devices have constrained computing power. Thus developers of these devices are limited to use as much as possible for the implementation of functions, not having enough space for securing its communication. This article focuses on how to possibly secure these communications.

Keywords: Narrowband, IoT, post-quantum cryptography, AES, NewHope

1 ÚVOD

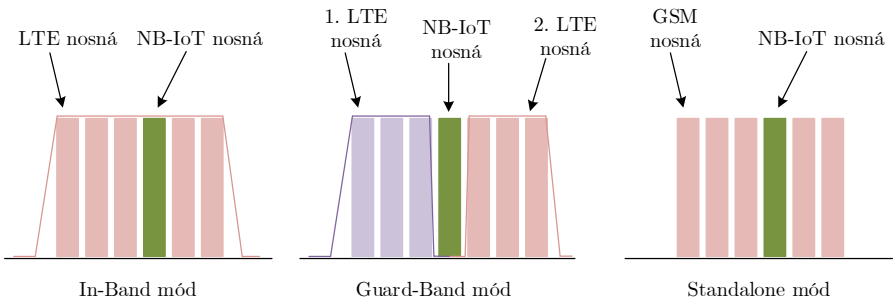
S neustále narůstajícím vývojem zařízení v Internetu věcí také souvisí problém udržení úrovně bezpečnosti probíhající komunikace. Toto není vyjímkou ani pro kontinuálně se rozšiřující škálu nízkoodběrových technologií LPWAN (Low-Powered Wide Area Network) zařízení s komunikační technologií NB-IoT (Narrowband Internet of Things) [1]. Taková zařízení většinou disponují podstatně menším výpočetním výkonem v porovnání s běžnými zařízeními připojenými do počítačových nebo mobilních sítí. Díky této skutečnosti není tak jednoduché použití běžných zabezpečovacích algoritmů a protokolů, tudíž při vývoji této komunikační technologie nebyl kladen důraz na podobné aspekty zranitelnosti.

Narrowband IoT je bezdrátová úzkopásmová technologie založená na komunikačních technologiích GSM a LTE, vyvinutou partnerským projektem 3GPP. Tento fakt ji dělá zajímavou volbou pro všechny, kteří se chtějí zapojit do světa Internetu věcí. Operátoři mají snadnou implementaci takového řešení do již stávající infrastruktury mobilních sítí právě kvůli tomu, že spolupracuje s technologiemi GSM a LTE. Zájemci o koncová zařízení s NB-IoT moduly jistě ocení jejich výborné charakteristiky jako například nasazení ve velkém měřítku v rámci relativně malého prostoru, dlouhou výdrží baterie, velkého rozsahu pokrytí a propustnostní signálu pevnými překážkami [1]. Tato řešení však nejsou koncipována tak, aby zajistila důvěryhodnost nebo integritu uživatelských dat, která se v síti přenáší. Pokud se zákazník rozhodne pro nasazení NB-IoT modulů přes službu, kterou by poskytoval operátor, tak v tomto případě data chráněna budou, jenže za cenu, že tato data spravuje třetí strana. Pokud na druhou stranu zákazník zvolí implementovat vlastní řešení jen za pomocí nákupu NB-IoT modulů a příslušných senzorů, vysílaná uživatelská data nejsou nijak chráněna.

2 NARROWBAND IOT

NB-IoT vyniká několika vlastnostmi a charakteristikami. Pomocí úsporného režimu (PSM) a rozšířenému nespojitému vysílání (eDRX) může být uskutečněna dlouhá pohotovostní doba. Celý vývoj NB-IoT je založený na základním LTE přenosu, který je upravený podle vlastností NB-IoT. Šířka

pásma na fyzické vrstvě je 200 kHz. V Evropě využívá frekvenčních pásem 800/900/1800 MHz pásma LTE [1]. V současné době podporuje NB-IoT jen polo-duplexní FDD se šířkou pásma 180 kHz, umožňující 3 typy nasazení (obrázek 1) – Stand-alone mód – zužitkovává nezávislé frekvenční pásmo mimo LTE pásma, pak Ochranné pásmo – Zužitkovává ochranné pásmo LTE, čemuž se rozumí čas, kdy je LTE pásmo v klidu, a nebo pracuje přímo v pásmu LTE – Pracuje kolektivně v pásmu LTE a zabírá jeden fyzický zdrojový blok frekvence pásma LTE.



Obrázek 1: Režimy nasazení NB-IoT.

2.1 Protokoly NB-IoT

Protokolová sada NB-IoT z větší části přejímá protokolovou sadu LTE, jen trochu zjednodušeně, aby splňovaly podmínky vlastností zařízení NB-IoT. Protokoly jsou poté následující:

- **NAS (Non Access Stratum)** – Nejvyšší vrstva skupiny protokolů NB-IoT a je používaná pro navázání IP spojení mezi koncovým zařízením a infrastrukturou sítě. NAS je tedy signalizační vrstva komunikace mezi koncovým zařízením (UE – User Equipment) a MME (Mobile Management Entity – server zpracovávající požadavky koncového zařízení ohledně komunikace v síti), zajišťující autentizaci zařízení do sítě, ustanovení klíčů používaných v komunikaci a výměnu parametrů potřebných pro komunikaci se sítí Internet.
- **RRC (Radio Resource Control)** – Protokol RRC slouží k registrování a následnému ustanovení připojení zařízení do mobilní sítě pomocí tzv. LTE Attach procedury. Různé RRC zprávy také stanovují různé signalizační rádiové nosiče – Signaling Radio Bearer (SRB). SRB popisuje způsob, jakým jsou data přenášeny z koncového zařízení do Internetu.
- **PDCP (Packet Data Convergence Protocol)** – Z hlediska základních operací je to, co dělá PDCP, velmi jednoduchý protokol – jen přidává PDCP hlavičku k příchozím datům a předá je RLC na downlinku, nebo právě naopak odstraňuje PDCP hlavičku od příchozího paketu a předává ji dále vrstvě IP v případu uplinku [2].
- **RLC (Radio Link Control)** – Radio Link Control je protokol druhé vrstvy a jeho prací je zajistit korektnost vysílaných dat a kvalitu rádiového kanálu. Stanovuje parametry komunikace přes rádiové rozhraní jako např. nastavení velikosti okna přenosu, časovač dotazování nebo maximální počet opakovaného poslání protokolové datové jednotky [2]. Protokol RLC je velice podobný protokolu SR-ARQ (Selective Repeat Automatic Request).

Největší slabinou NB-IoT ale je, že komunikuje přes nespolehlivý protokol UDP. Důvodem je, že zařízení nemůže použít transportní protokol TCP, jelikož si nemůže dovolit čekat na odpověď zdali zařízení, se kterým komunikuje, opravdu zprávu obdrželo, což TCP protokol vynucuje. Jak již bylo

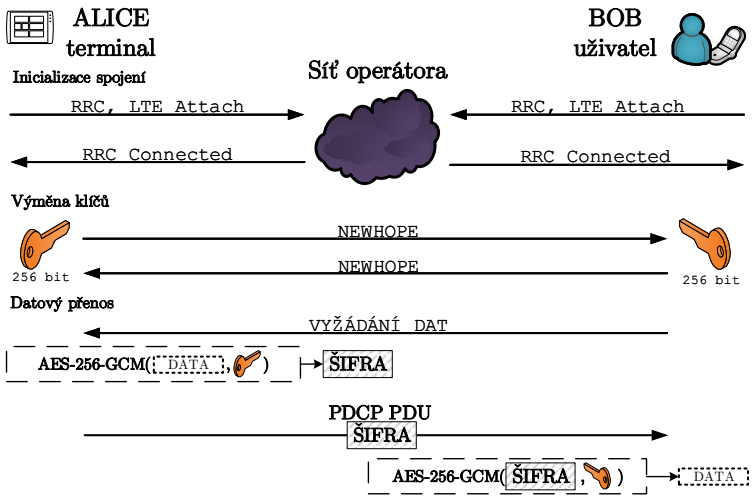
nastíněno v úvodu, nasazení senzorů s využitím služeb operátora má dvě slabiny z pohledu bezpečnosti komunikace. V síti operátora je, samozřejmě, komunikace zabezpečena, ale může být teoreticky odposlouchávána operátorem v extrémních případech. Druhou slabinou je poté to, že jakmile data opustí infrastrukturu operátora, tak jsou vyslána v otevřené podobě přes Internet až ke koncovému zařízení, které si vyžádalo data.

3 NÁVRH END-TO-END ZABEZPEČENÍ NB-IOT

V dnešní době se kryptografie zaměřuje hlavně na dva matematické problémy, jmenovitě problém faktorizace a problém diskrétního logaritmu. Tyto matematické problémy jsou hojně využívány v dnešních kryptografických algoritmech, ať už je to RSA, DSA, či ECDH. V roce 1994 ale Peter Shor, americký profesor aplikované matematiky na MIT, přišel na způsob, jakým lze tyto problémy vyřešit pomocí kvantových počítačů, kvantové Fourierovy transformace, modulárního a binárního umocňování [3]. Tím se dnešní algoritmy stávají doslova nepoužitelnými v budoucnosti. Na řadu tedy přišly algoritmy, které využívají jiných matematických problémů, u kterých není zatím známo, že by byly řešitelné v dostačujícím čase. Post-kvantová kryptografie tedy implementuje řadu jiných matematických problémů, jako například mřížky, hashovací funkce, supersingulární isogenní eliptické křivky nebo také polynomiální rovnice.

V běžně zabezpečené elektronické komunikaci je v prvé řadě za potřebí stanovit sdílený klíč mezi komunikujícími zařízeními, a proto byl z této oblasti vybrán algoritmus NewHope. Tento algoritmus je jedním z nových post-kvantových algoritmů, který byl predložen na soutěži post-kvantových algoritmů vyhlášené organizací NIST v roce 2016. Vychází z protokolu BCNS, který je založený na problému R-LWE (Ring-learning-with-errors) a autoři NewHope se snažili napravit chyby tohoto algoritmu a zefektivnit jej. Například používá mřížku D_4, která umožňuje snížit modulo na $q = 12289 < 2^{14}$, parametr a (veřejný parametr znám oběma stranami) se teď generuje nově při každém ustanovení klíčů nebo při distribuci chyb nahrazuje diskrétní Gaussovo rozložení za binomické rozložení, jehož střední hodnota je 0 a rozptyl $k/2$, které je mnohem efektivnější [4].

Poté co je stanovený sdílený klíč, mohou zařízení komunikovat v podobě šifrovaných zpráv. Pro tuto úlohu byl zvolen šifrovací algoritmus AES se šifrovacím klíčem o velikosti 256 bitů v operačním módu GCM. Pomocí AES tedy budeme šifrovat uživatelská data, která vytvoří senzor. Tyto data poté budeme přenášet přes NB-IoT síť až k uživateli, který musí mít tedy pochopitelně stejný šifrovací klíč, který byl vložen do blokové šifry, aby mohl tyto data dešifrovat. Celý proces poté znázorňuje obrázek 2.



Obrázek 2: Návrh zabezpečení NB-IoT komunikace.

4 REALIZACE NÁVRHU

K uskutečnění našeho návrhu budeme používat zařízení s omezeným výkonem, konkrétně mikrokontrolér ATmega2560, společně se shieldem, na kterém je umístěn NB-IoT modul SARA-N210. Arduino Mega 2560 je vývojová deska, která umožňuje vymýšlet nové prototypy na mikrokontroléru ATmega2560. Disponuje také kolíkovými lištami, které umožňují přístup ke vstupním a výstupním periferiím mikrokontroléru. Dá se na ně také připojit velká škála tzv. shieldů, které dodávají různou funkcionalitu vývojové desce od senzorů teploty až po měřiče kvality ovzduší, aj. Na kontrolér je připojený shield s NB-IoT modulem SARA-N210 vyráběný firmou ublox, konkrétně verze 01B-00.

Pro práci se SARA modulem jsou využívány tzv. AT příkazy, které ovládají různé funkce tohoto modulu, jako například zapnutí/vypnutí, registraci zařízení do sítě nebo odeslání či přijmutí zpráv. Jelikož mikrokontrolér disponuje pouze 8 KB operační paměti, byly zde určité obavy s nedostupností místa při implementaci obou algoritmů, NewHope a AES, na takové zařízení. Současný stav vývoje ale poukazuje, že algoritmus NewHope zabírá kolem 30% a AES poté jen dalších 11%. S dalšími funkcemi, jako například interní logika s připojováním k základnové stanici, registraci zařízení do sítě a odeslání zašifrované zprávy, je očekáváno, že při vyvinuté funkcionalitě bude využito maximálně 70% operační paměti zařízení Arduino Mega 2560. Ze současného stavu návrhu bylo také možné zjistit jak se projeví zpoždění konverzace při nasazení algoritmu pro stanovené klíče a šifrování na mikrokontroléru. S testovanou délkou zprávy 16 bajtů (resp. 128 bitů) jsme mohli z celkových patnácti měření zaznamenat průměrné zpoždění 1281792 μs (1,28 sekundy). Toto měření zahrnuje generaci veřejného klíče, generaci sdíleného klíče a zmíněné zašifrování 16 bajtů dat.

5 ZÁVĚR

Článek poukazuje na to, že některé nové technologie nejsou vymyšlené do úplného konce a je tak tedy za potřebí druhého pohledu na věc. Bylo dokázáno, že data přenášená úzkopásmovou komunikační technologií nejsou nijak chráněna proti potencionálnímu útočníkovi. Hlavním cílem článku je shrnutí jak by se taková skutečnost dala napravit pomocí implementace novodobých kryptografických algoritmů a tím sestavit tak robustní systém zabezpečení pro takové technologie. Současně rozpracovaná bakalářská práce bude poté testovat dopad vyvinuté funkcionality na odběr nízko-odběrových zařízení a tím také dopad na celkovou výdrž zařízení nápájenými pouze tužkovými baterkami.

REFERENCE

[1] M. CHEN, Y. MIAO, Y. HAO a K. HWANG. *Narrow Band Internet of Things*. IEEE Access [online]. 2017, 5, 20557-20577 [cit. 14. 3. 2019]. DOI: 10.1109/ACCESS.2017.2751586. ISSN: 2169-3536.

[2] M. PRADHAN, Nex-G *Narrow Band Internet of Things (NB IoT)* [online], publikováno 1. 9. 2017, [cit. 14. 3. 2019].

[3] NAGAICH, Shweta a Y.C. GOSWAMI. *Shor's Algorithm for Quantum Numbers Using MATLAB Simulator*. In: 2015 Fifth International Conference on Advanced Computing & Communication Technologies [online]. IEEE, 2015, 2015, s. 165-168 [cit. 18. 11. 2018]. DOI: 10.1109/ACCT.2015.16. ISBN 978-1-4799-8488-6.

[4] E. ALKIM, L. DUCAS, T. PÖPPELMANN, P. SCHWABE *Post-quantum key exchange - a new hope* [online], publikováno 10. 11. 2015, citováno 12. 11. 2018.